Data-Security / Data-Protection

Datenschutz (Data-Protection)

Schutz von sensitiven Daten vor…

- anderen Personen
- Verlust von Datenträgern

Datenschutz bei Datenaustausch

Daten können bei Uebermittlung...

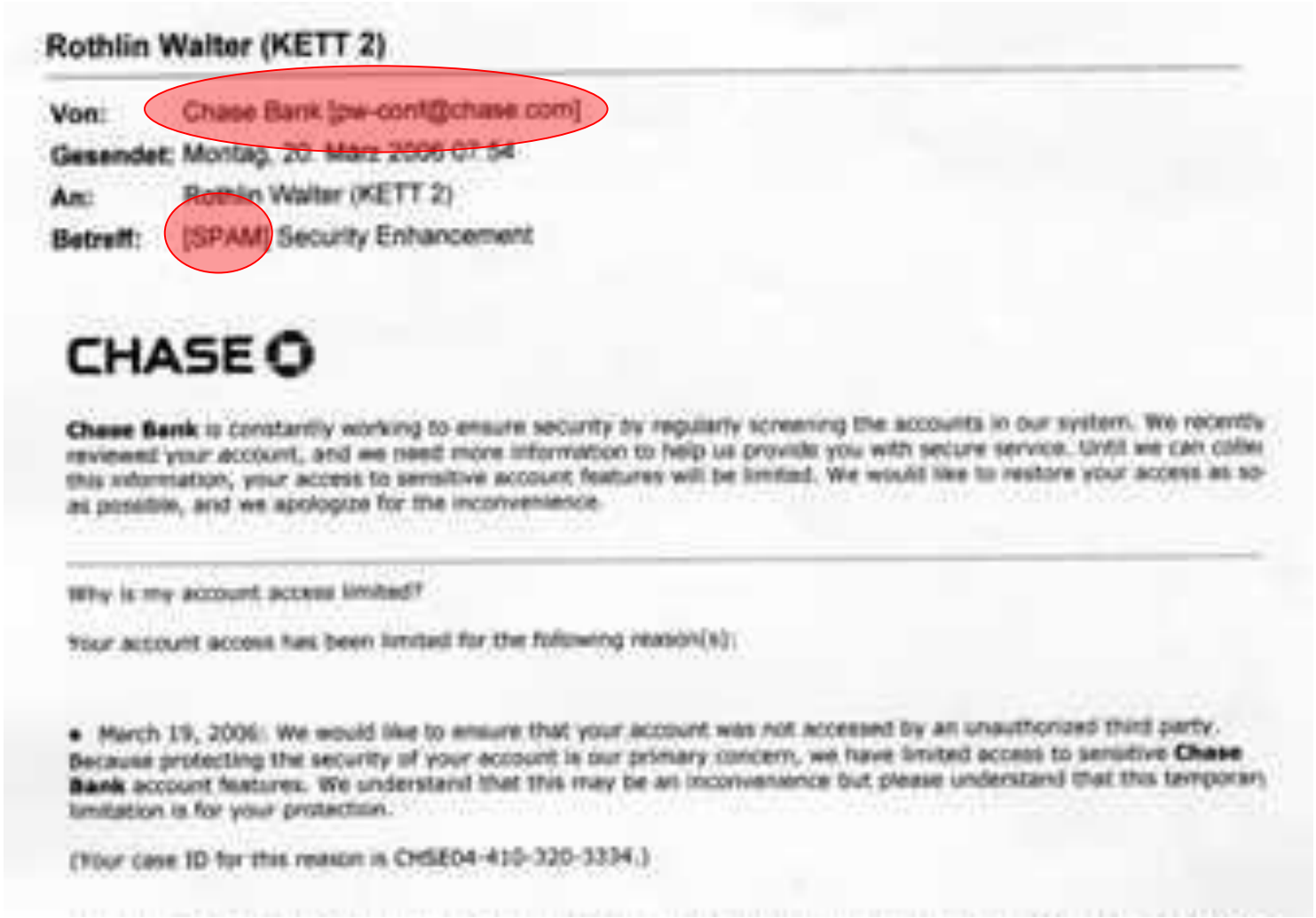
- Mitgelesen werden (Kopien)
- Verfälscht werden

Authentifikation

Ist Absender / Empfänger wirklich die Person die ich meine?

- Wie erkenne ich jemanden am Telefon?
- Wie bin ich sicher, dass eine e-mail mit Absender Walter@Rothlin.com wirklich ER ist?

Authentifikation



Rothlin Walter (KETT 2)

Von: Chase Bank [pw-cont@chase.com]
Gesendet: Montag, 20. März 2006 07:54
An: Rothlin Walter (KETT 2)
Betreff: [SPAM] Security Enhancement

CHASE

Chase Bank is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

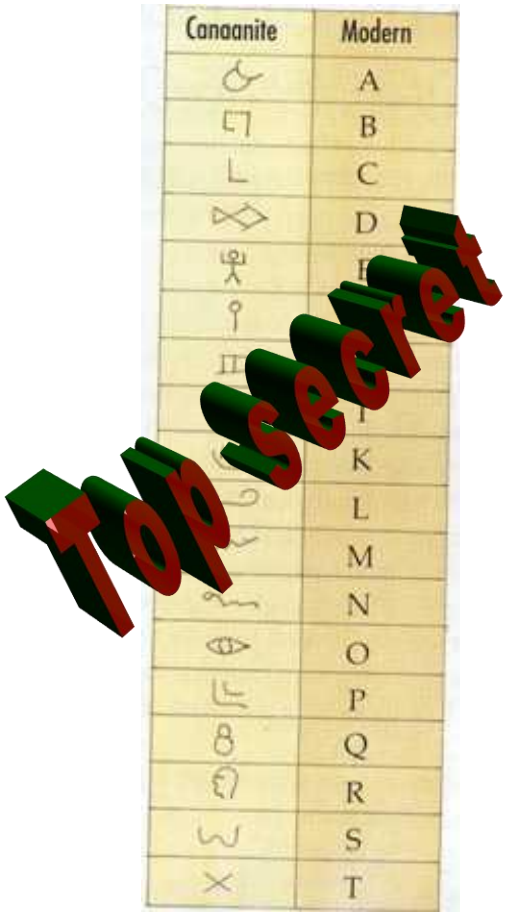
Why is my account access limited?

Your account access has been limited for the following reason(s):

- March 19, 2006: We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive **Chase Bank** account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

(Your case ID for this reason is CHSE04-410-320-3334.)

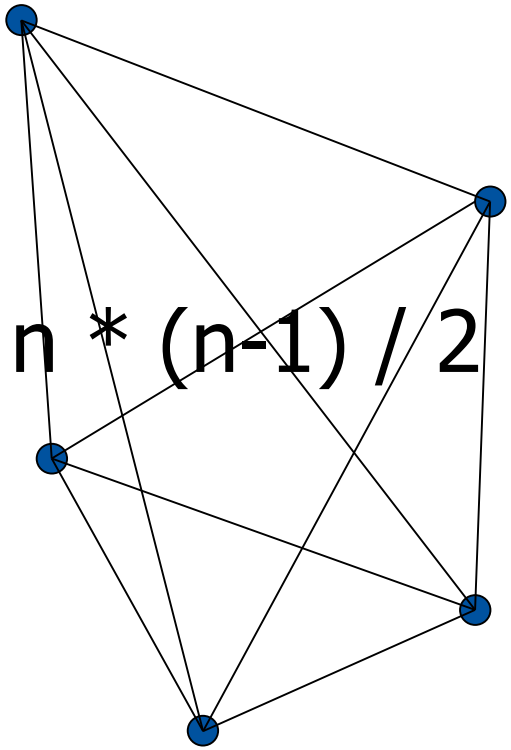
Verschlüsselung (symmetrisch)



Sender und Empfänger vereinbaren, wie verschlüsselt wird.

Schlüsselaustausch ist das Sicherheitsproblem

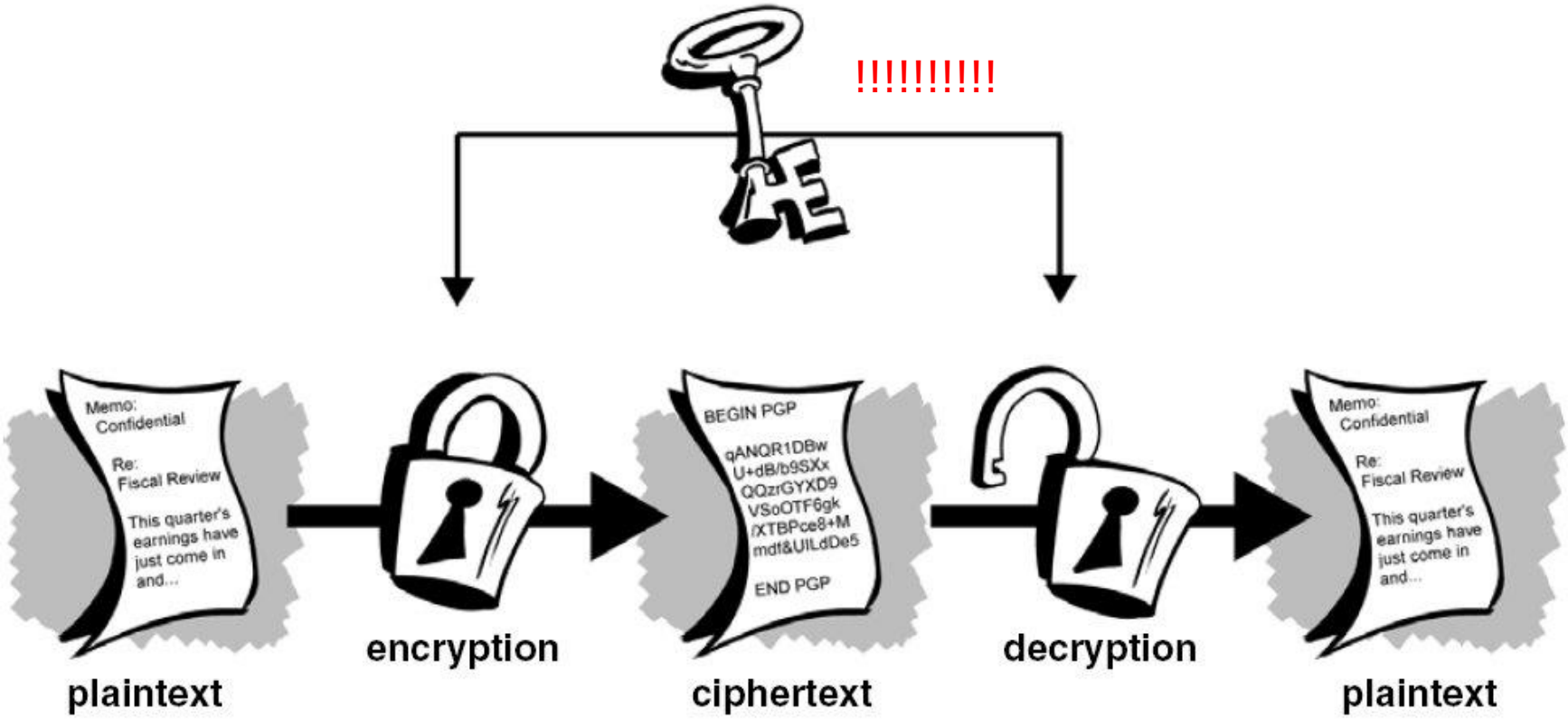
Verschlüsselung (symmetrisch)



Es benötigt pro Verbindung einen Schlüssel!

Schlüsselverwaltung + Schlüsselaustausch problematisch

Verschlüsselung (symmetrisch)



Verschlüsselung (asymmetrisch)

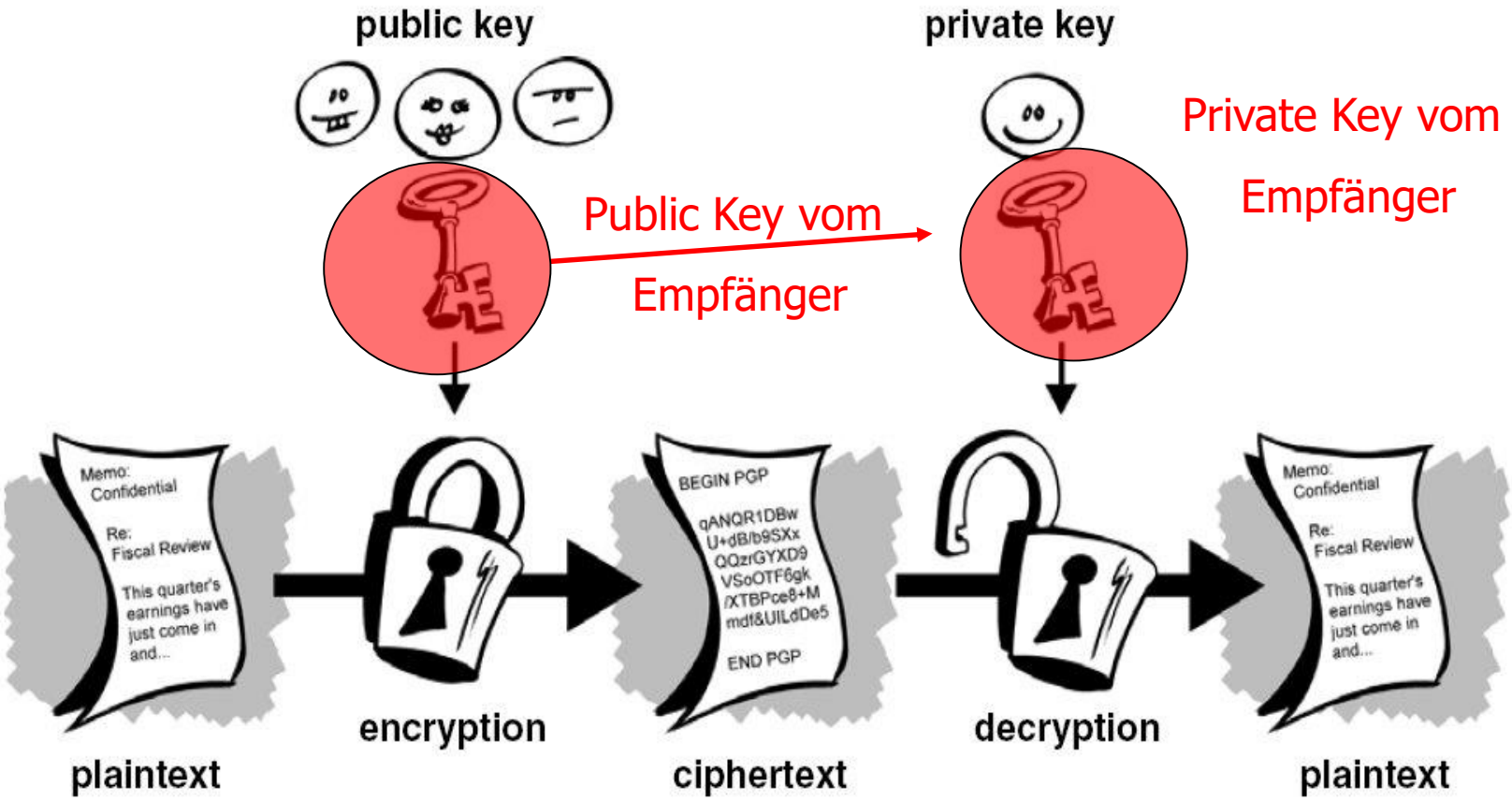
Jeder Kommunikationspartner hat einen
Public- und einen Private-Key

Verschlüsselt wird mit dem
Public-Key des Empfängers

Entschlüsselt wird mit dem
Private-Key des Empfängers

Verschlüsselung (asymmetrisch)

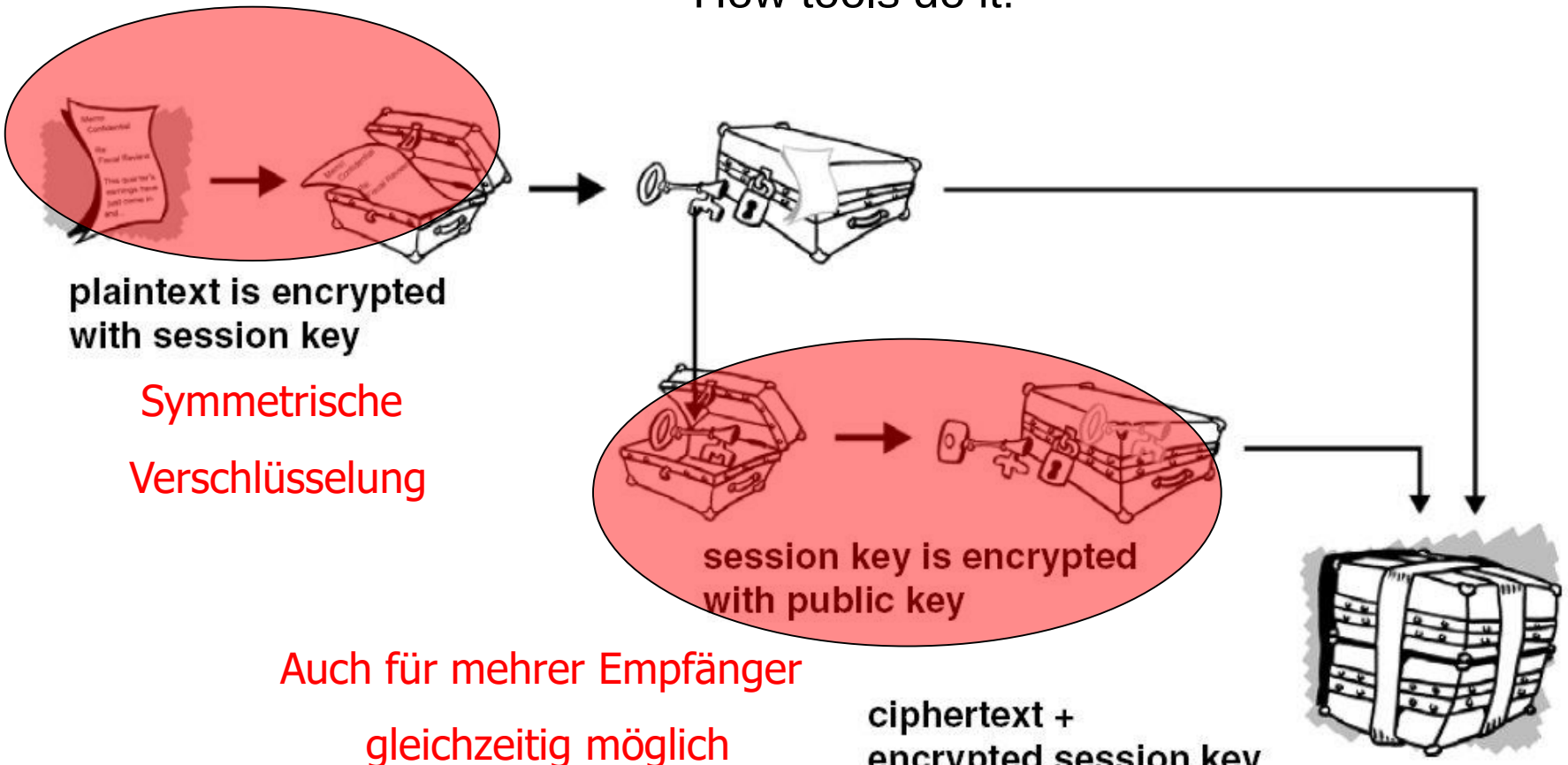
Public – Private Key Encryption (PPK)



HWZ | Hochschule für Wirtschaft Zürich

Verschlüsselung (asymmetrisch)

How tools do it!



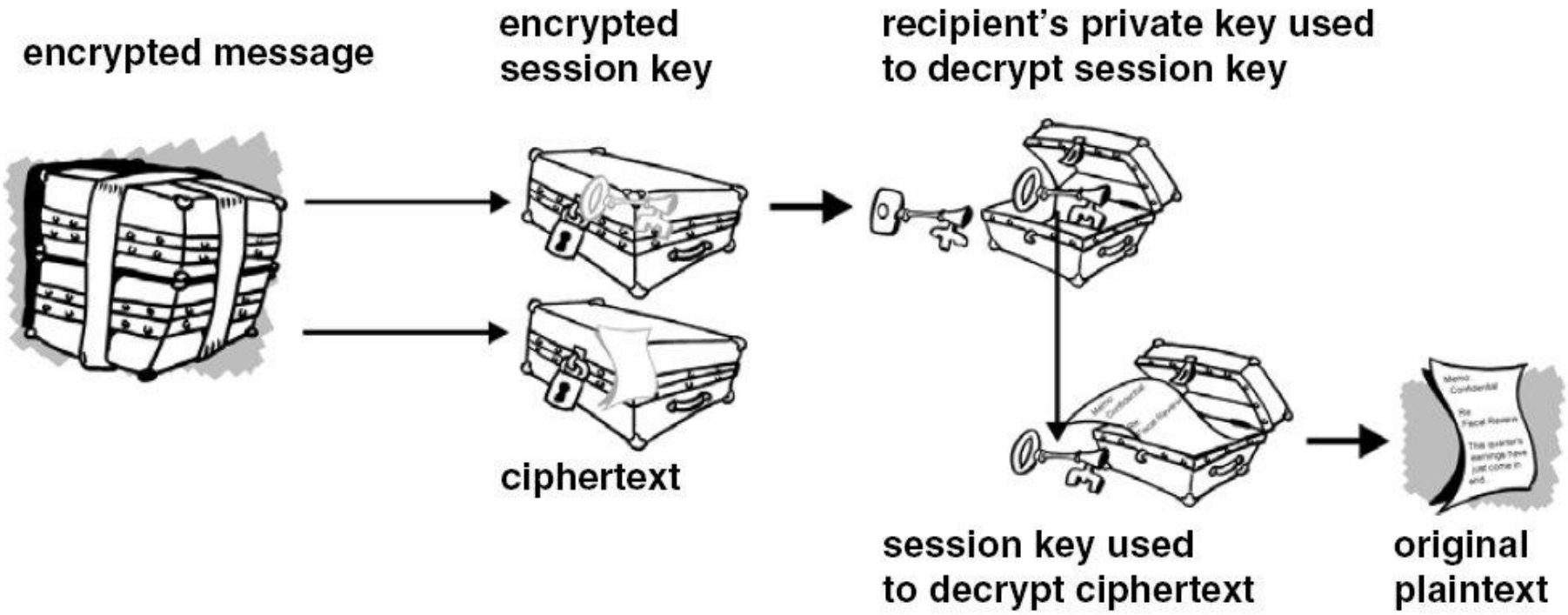
Symmetrische

Verschlüsselung

Auch für mehrer Empfänger

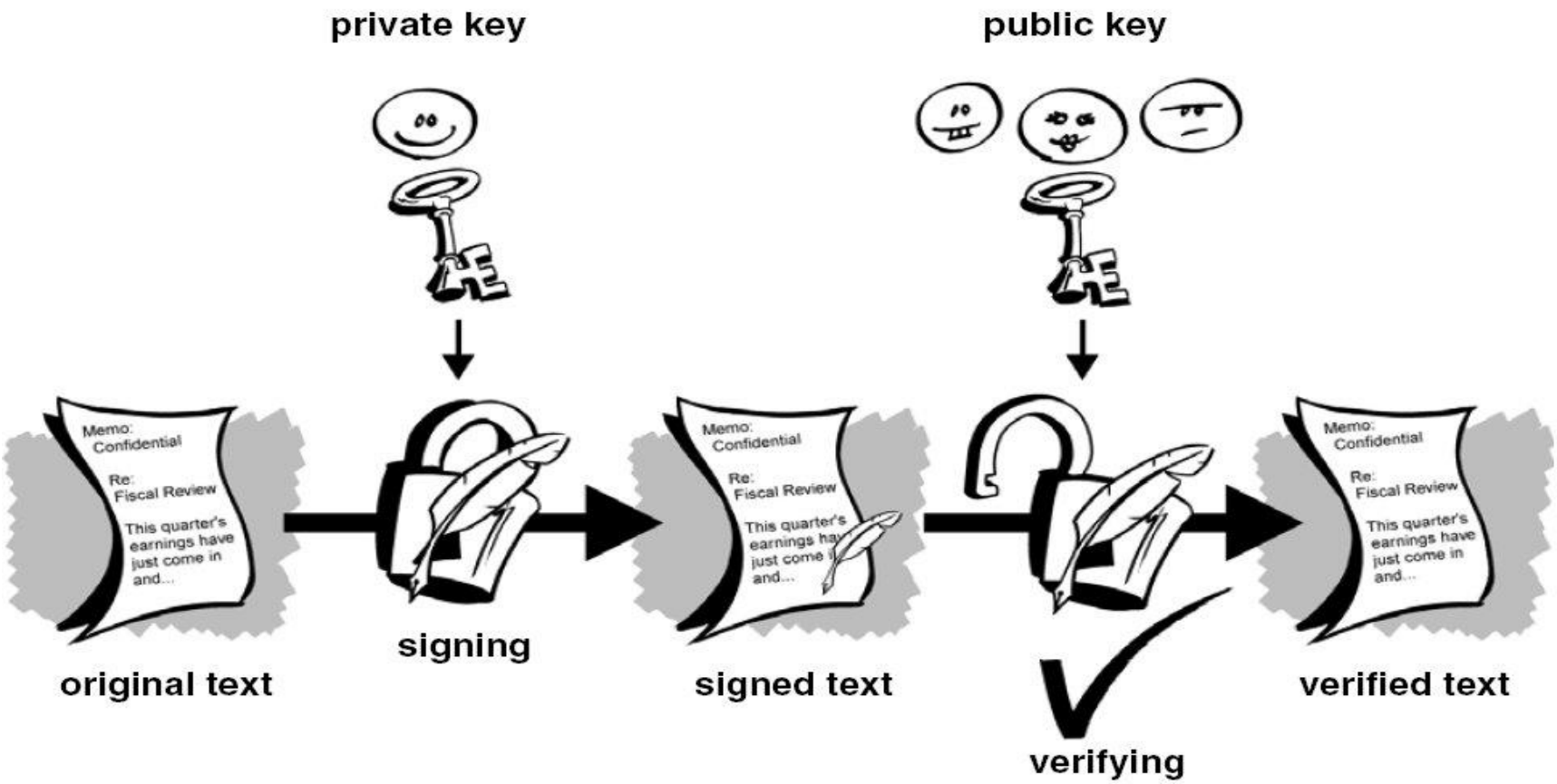
gleichzeitig möglich

Verschlüsselung (asymmetrisch) How tools do it!

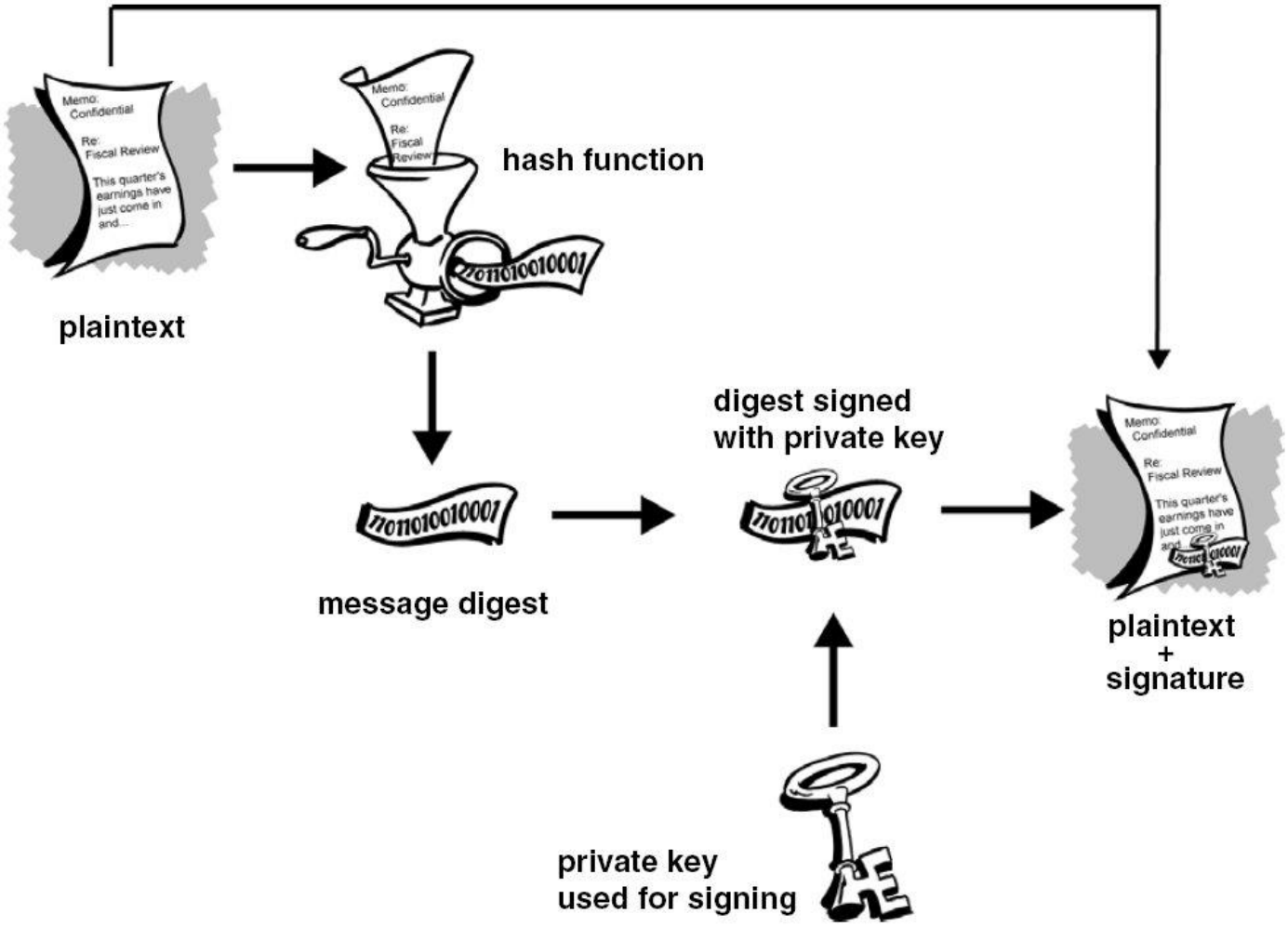


Visieren (Signing)

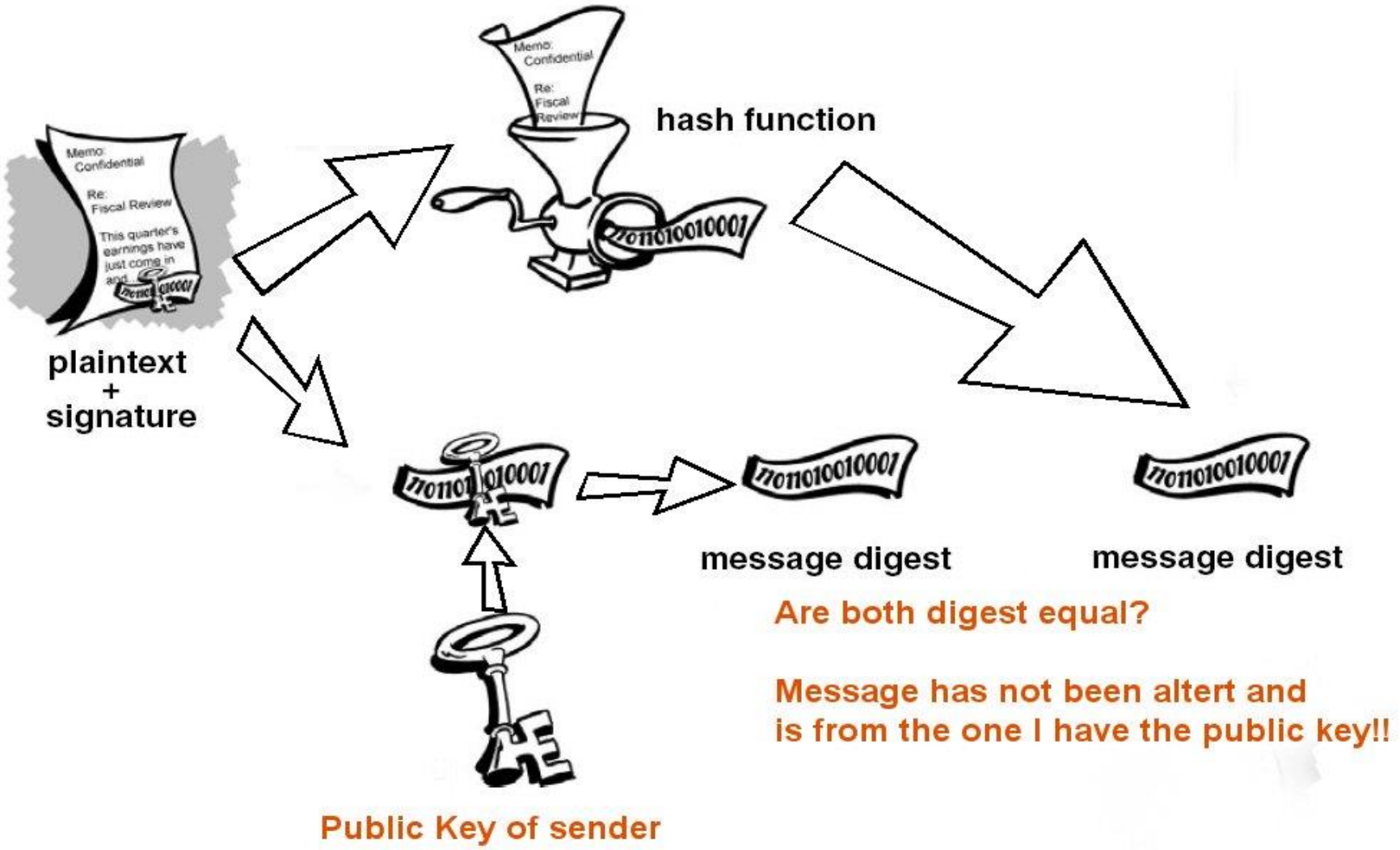
Private Key kann auch für Verschlüsselung verwendet werden!



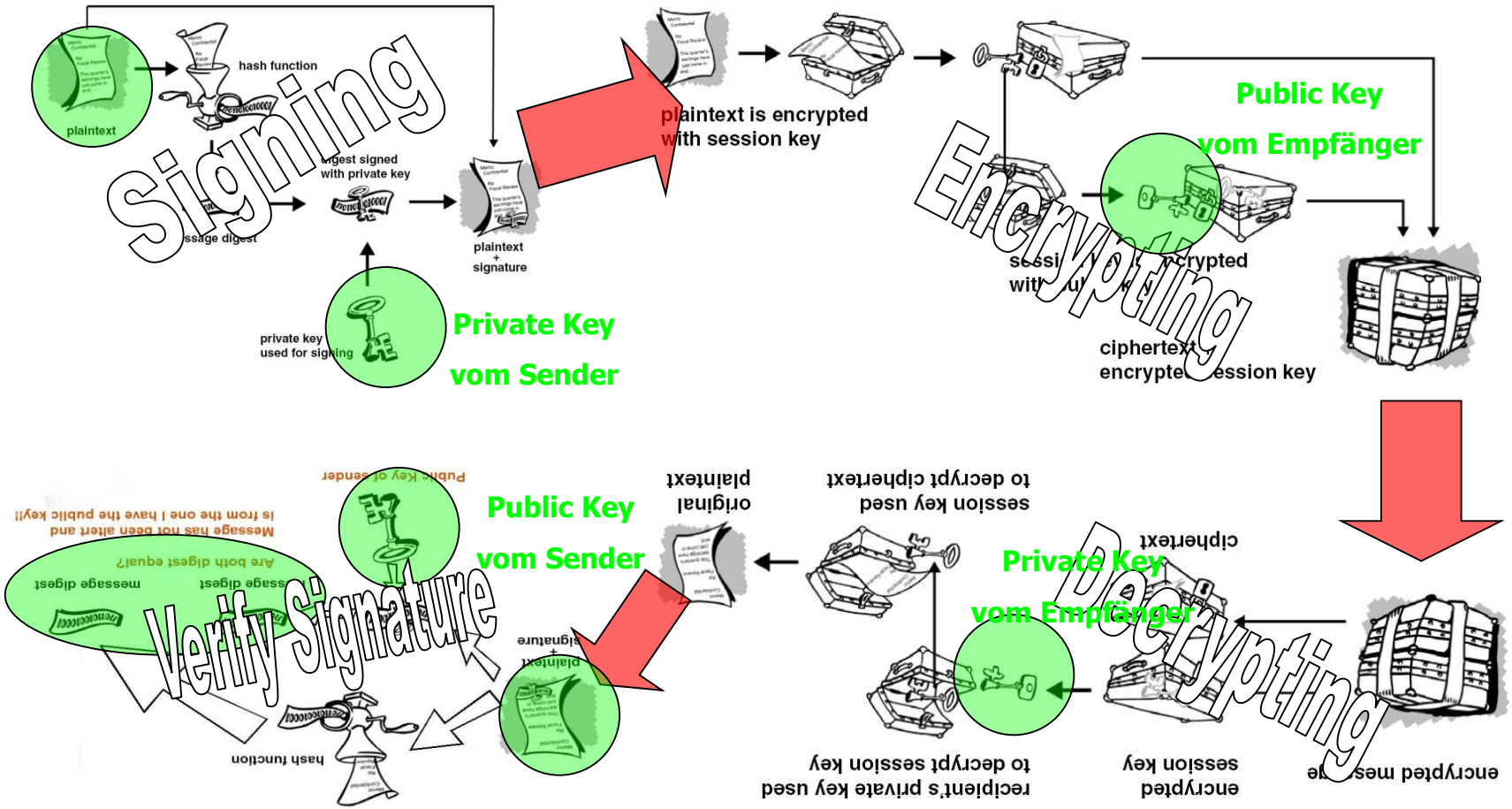
Visieren (Signing) How tools do it!



Visieren (Verifizieren)



Visieren und Verschlüsseln



Anforderungen an Sicherheit und deren Erfüllung

Vertraulichkeit (confidentiality)

- Bsp. Aktien-Kauf: *Finanzamt soll aber nicht erfahren, was ich mit Aktien mache*
- Kommunikationsflüsse beschränken/absichern

Integrität

- *keine Fälschung „Verkauforder“ zu „Kauforder“*
- Unautorisierte Manipulation verhindern

Authentizität

- *Bank und ich wollen gegenseitig wissen, wer was macht – wo landet denn mein Geld?*
- Eindeutige Identifikation der Subjekte

Verbindlichkeit (non-repudiation)

Verfügbarkeit

Anonymität

Sicherheitsmechanismen & -verfahren: Realisierung

Vertraulichkeit

- Kryptographische Verfahren: symmetrische, asymmetrische, z.B. DES, (AES), IDEA, Twofish, RC4, A3, A5, A8, RSA, El-Gamal
- Sicherheitsklassifikation (labeling) & Beschränkungen, z.B. Bell LaPadula: no-read-up, no-write-down

Authentizität

- Wissensbasiert: Passwortverfahren, Challenge-Response, Message Authentication Codes (MAC), Passworte z.B. S/KEY, PINs; Zertifikate z.B. X.509, MAC-Verfahren z.B. MD5, HMAC-MD5
- Besitzbasiert: Chipkarte, Smartkarte z.B. SIM-Karte in GSM
- Biometrie: Fingerabdruck, Iris-, Retina-Scanner etc.

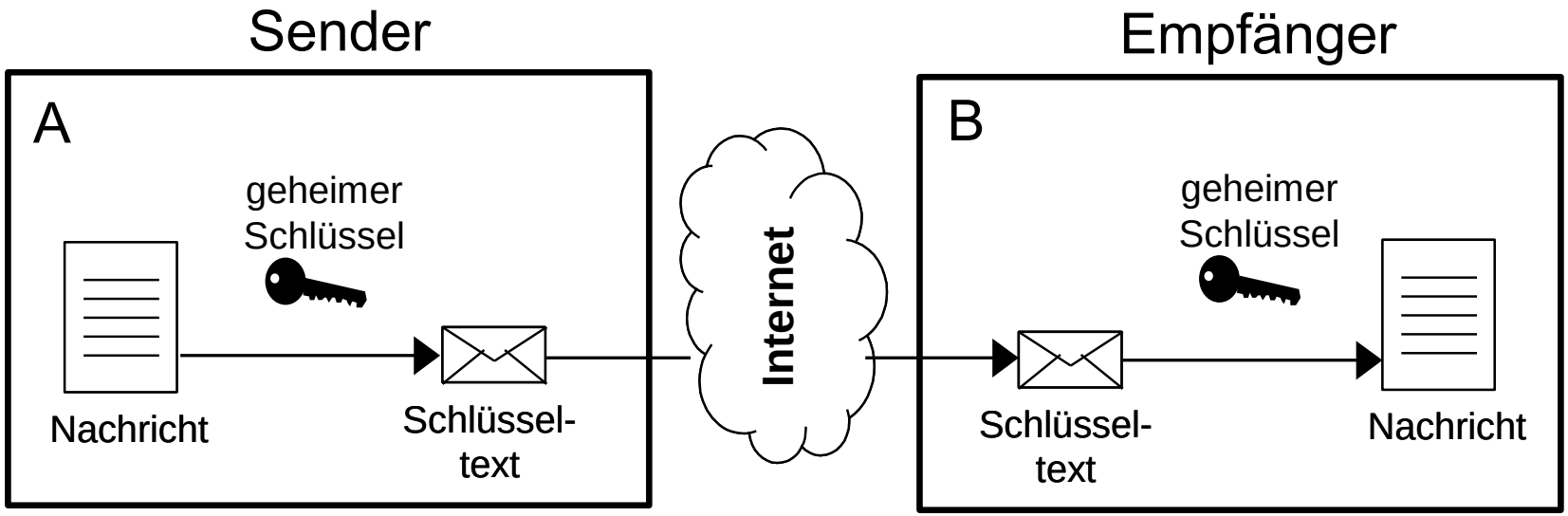
Datenintegrität

- Hashfunktionen, Prüfsummen: z.B. MD5, SHA-1
- Zugriffskontrollisten ACL, Capabilities, Zugriffstickets

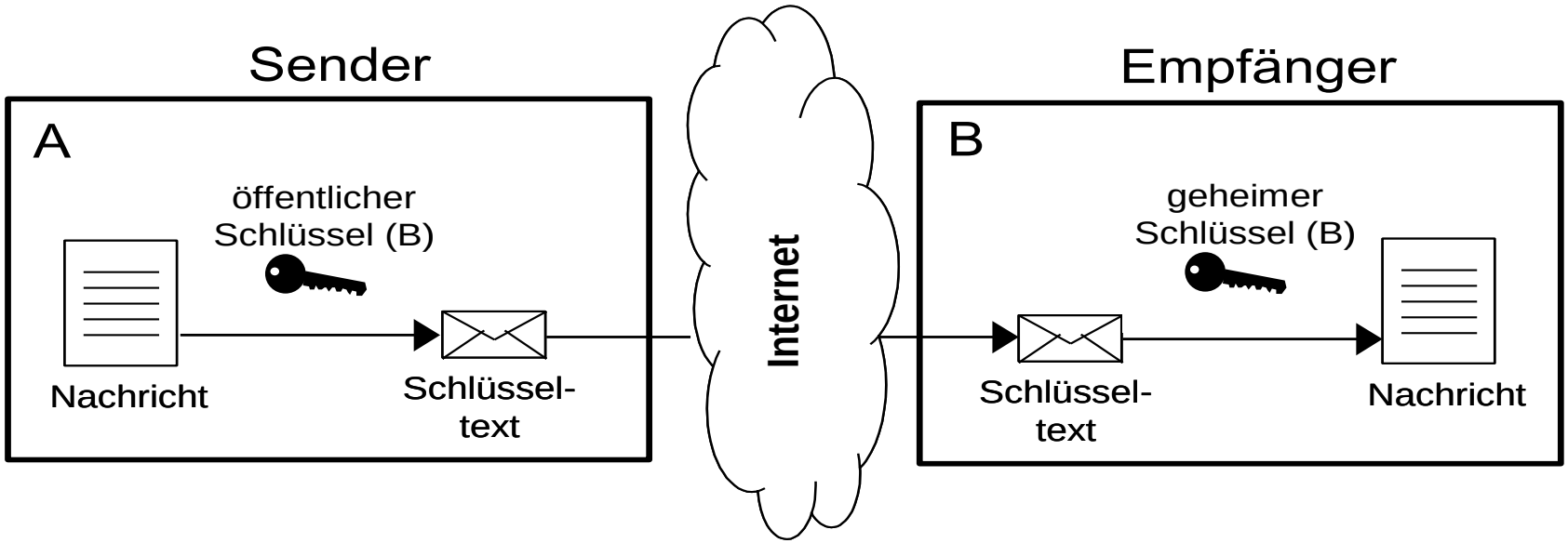
Verbindlichkeit: digitale Signaturen: z.B. DSA, RSA

Verfügbarkeit: Netzüberwachung, Filterungen

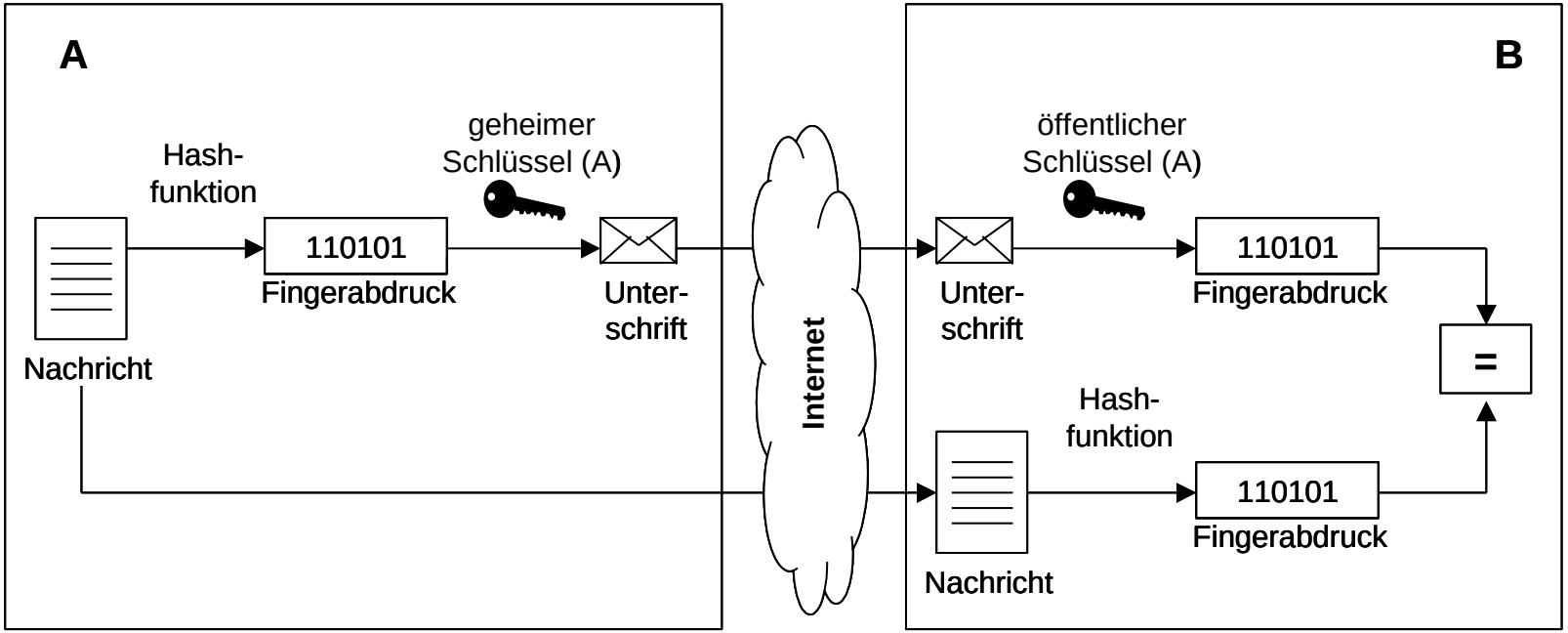
Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung



Digitale Signatur

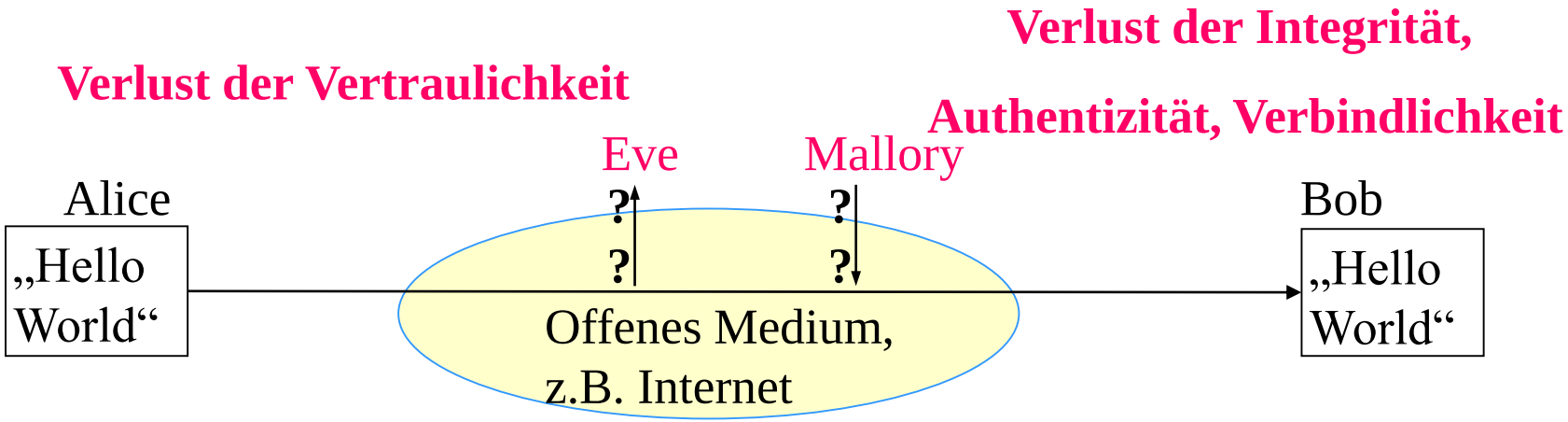


Ausgangslage für Kryptosysteme

Alice will Bob eine Nachricht schicken,

Eve soll den Inhalt der Nachricht nicht erfahren (Vertraulichkeit)

Mallory soll keine Chance haben, den Inhalt der Nachricht unerkannt zu verfälschen oder falsche Nachrichten abzuschicken (Integrität und Authentifizierung).



Ablauf einer verschlüsselten Kommunikation

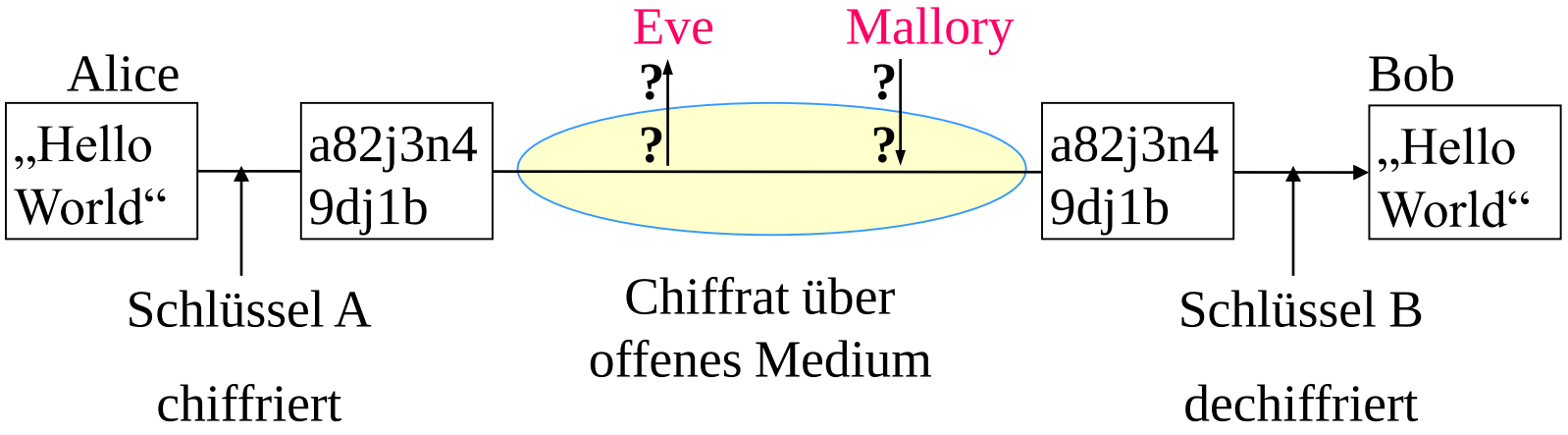
Alice **verschlüsselt / chiffriert** Nachricht („**Klartext“)** mit Hilfe ihres **Schlüssels** und einer **Verschlüsselungs-** oder auch **Chiffrierfunktion**.

Alice schickt **Chiffrat** / **Kryptogramm** an Bob

Bob nutzt eigenen Schlüssel und eine **Entschlüsselungs-** oder **Dechiffrierfunktion** zur Umwandlung in Klartext

Idealfall

- Eve kann mit Chiffrat die ursprüngliche Nachricht nicht erlangen
- Eine Änderung durch Mallory fällt Bob sofort auf



IDEA (International Data Encryption Algorithm)

symmetrische Blockchiffre, Blocklänge 64 Bit, feste Schlüssellänge 128 Bit.

Ver- und Entschlüsselung:

- gleicher Algorithmus
- Dechiffrierschlüssel leicht aus Chiffrierschlüssel zu bestimmen.

Hilfsmittel

- Erzeuge 52 Unterschlüssel, indem man den 128 Bit langen Schlüssel in acht 16 Bit lange Unterschlüssel zerteilt.
- Die nächsten 8 Unterschlüssel erhält man, indem man die Bits des Schlüssels um 25 Positionen nach links rotiert und dann den Schlüssel in acht Segmente zerteilt und so weiter.

Asymmetrische Kryptosysteme – allgemeiner Ablauf

Kommunikationspartner Alice & Bob erzeugen sich jeweils ein Schlüsselpaar (ek_{alice}, dk_{alice}) bzw. (ek_{bob}, dk_{bob})

- ek Schlüssel: öffentlich (in ein Verzeichnis)
- dk Schlüssel: geheim

Alice **verschlüsselt** M mit dem öffentlichen Schlüssel ek_{bob} von Bob: **$C = enc(M, ek_{bob})$**

Versenden der Nachricht C von Alice zu Bob

Bob **entschlüsselt** C mit seinem privaten Schlüssel dk_{bob} : **$M = dec(C, dk_{bob})$** = $dec(enc(M, ek_{bob}); dk_{bob})$

Anwendungen – sicherer Transfer: SSL

SSL (Secure Socket Layer): kryptographisch gesicherte Übermittlung von Informationen im Internet

Wichtige Aspekte

- 40-bit SSL unsicher => 128-bit zu bevorzugen
- **Hybrides Verfahren**
  - Zuerst RSA
  - Dann symmetrisches Verfahren: höheren Geschwindigkeit dieser Kryptosysteme. (Sonst zusätzliche Transaktionskosten).
- RSA: Schlüssel mehrfach, daher höhere Sicherheit. Symmetrisches Verfahren: nur für den Schutz einer Übertragung.

Anwendung: Erzeugung und Nutzung Digitale Signatur

Eigenschaften handschriftlicher Unterschriften auf digitale Welt übertragen

Probleme: u.a. leichtes Ausschneiden, Kopieren, Verfälschen digitaler Muster

- **Signaturerstellung** meist mit **asymmetrischen** Verfahren
- Idee: Alice signiert mit dem privaten, geheimen Schlüssel ek_{alice} : sig = dec(M, dk_{alice})
- Verifikation der Signatur mit zugeordnetem öffentlichen Schlüssel: M = enc(sig; ek_{alice})

- Gewährleistung von Authentizität und Vertraulichkeit

  1.Verschlüssele mit öffentlichen Schlüssel des Empfängers

  2. Verschlüssele mit geheimen Schlüssel des Senders (s.o.)

Zertifikate

Problem: Authentizität des öffentlichen Schlüssels ek_{alice} zusichern!

Benötigt: Vertrauenswürdige Instanz (CA) (Trust Center, Certification Authority): signiert ek_{alice} mit dk_{ca}

Problem: Authentizität von ek_{alice}! Das eigentliche Problem wurde deligiert…

Infrastruktur für Zertifikate notwendig: PKI Public-Key Infrastructure

Beispiel für ein Zertifikat: X.509 (Auszug)

- Versionsnummer — beschreibt verwendetes Zertifikatformat
- Seriennummer — eindeutiger Identifikator
- Signatur — verwendete Algorithmen und Parameter
- Zertifikataussteller — Name der ausstellenden Instanz
- Gültigkeitsdauer — Angabe eines Zeitintervalls
- Benutzername — eindeutiger Name des Benutzers

PKI - Schlüsselverwaltung

Public Key:

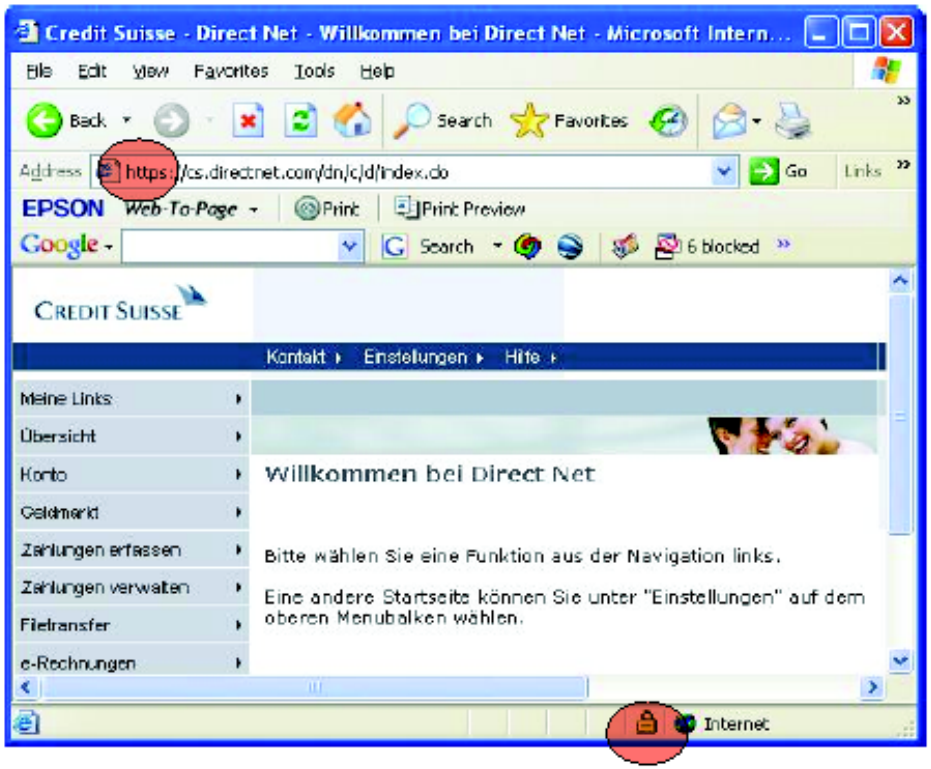
- URL für Download auf Visitenkarte
- Attached an jedes e-mail

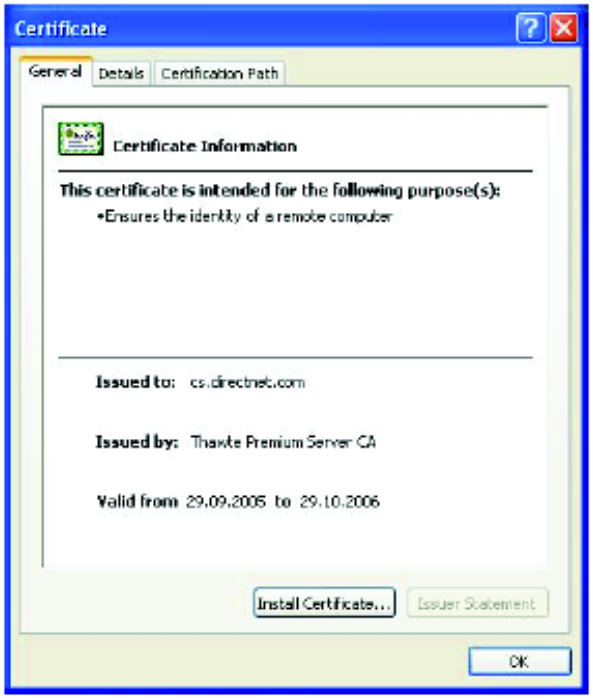
Private Key:

- Auf Computer Hard-Disk (Backup im Safe)
- Smartcard
- Cryptokey
- Mit einem Passwort geschützt

Public Key Zertifikate

- Bindet ein Public Key mit einer Identität zusammen
- Name, Geburtsdatum,... ist im Certificate
- Certificates werden von der Ausgabenstelle elektronisch visiert
- Ausgabenstelle: Certificate Authority (CA)
- SSL: Secure Socket Layer (https)





Sonstige Konzepte

- Strichlisten
- SecureID Card
- PKI: Public Key Infrastructure
- GPG (GNU Privacy Guard)
  - Open Source PGP
  - Download for Windows
    http://www.gpg4win.org/index.html

Viren, Würmer, Trojaner

- Alle drei können Daten zerstören oder Informationen weitergeben
- Viren hängen sich an eine Datei und werden durch kopieren dieser Datei verbreitet.
- Würmer nutzen einen Dienst vom Computer (e-mail, Netzwerkfunktionen) um sich selbständig auf andere Systeme zu kopieren.
- Trojaner (Trojanisches Pferd) gibt etwas anderes vor als es macht

Viren, Würmer, Trojaner

- Anti-Virus Software aktuell halten
  (Serum nachladen)
- Vorsicht beim Download und kopieren
- Misstraue jedem e-mail
- Windows um mehrfaches mehr gefährdet als
  LINUX, UNIX oder MAC

Firewall und Proxy-Server

- Firewall: Durch diese Gasse muss er kommen
- Regeln was erlaubt ist müssen definiert sein
- Genaues loggen was passiert

- Proxi: Stellvertreter
- Regeln was erlaubt und was verboten ist
- Genaues loggen aller Requests
- Cashing möglich

Verschlüsselt oder Unverschlüsselt

Lieber Chef! Mein Assistent, Herr Meyer, ist immer dabei,

seine Zeit mit Schwätzchen mit seinen Kollegen zu verplempern. Nie

schafft er sein Arbeitspensum; und sehr oft bleibt er länger

in der Mittagspause. Mein Assistent ist jemand ohne

Computerkenntnisse. Er ist einer der Mitarbeiter, auf die man

gern verzichtet. Ich denke, dass es Zeit wird für ihn,

zu gehen. Die Firma kann davon nur profitieren

Aber: am Ende steht immer der Mensch

- Zugriff für Unberechtigte vermeiden!
  Aufräumen, Abschliessen, Vernichten,
- Sich an Regeln halten und Weisungen befolgen!
  auch wenn immer alles problemlos ging
- Andere sensibilisieren es auch zu machen

➔ Wissen ist vorhanden. Am Machen scheitert es!